JOURNAL OF COMBINATORIAL THEORY, Series A **24**, 34–49 (1978)

Counting and Constructing Orthogonal Circulants

K. A. BYRD AND T. P. VAUGHAN

Department of Mathematics, University of North Carolina, Greensboro, North Carolina 27412

Communicated by the Managing Editors

Received August 12, 1976

If F is an arbitrary finite field and T is an $n \times n$ orthogonal matrix with entries in F then one may ask how to find all the orthogonal matrices belonging to the algebra $F[T]$ and one may want to know the cardinality of this group. We present here a means of constructing this group of orthogonal matrices given the complete factorization of the minimal polynomial of T over F. As a corollary of this construction scheme we give an explicit formula for the number of $n \times n$ orthogonal circulant matrices over $GF(p^l)$ and a similar formula for symmetric circulants. These generalize results of MacWilliams, *J. Combinatorial Theory* **10** (1971), 1–17.

INTRODUCTION

It is the purpose of this paper to develop a simple formula [see Sect. 4] for calculating the number of $n \times n$ orthogonal circulant matrices with entries from $GF(p^l)$ by methods which describe at the same time how these matrices may be constructed.

PRELIMINARIES

Let F be a field. An $n \times n$ circulant over F is a matrix of the form:

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{bmatrix},$$

where the entries a_i belong to F. If T is the circulant with $a_i = \delta_{i1}$, then the general circulant can be expressed as $A = \sum_{j=0}^{n-1} a_j T^j$. Thus the algebra of circulants is the subalgebra $F[T]$ of the algebra F_n of $n \times n$ matrices over F. Since the minimum polynomial of T is $\psi(x) = x^n - 1$ the algebra of

0097-3165/78/0241-0034$02.00/0

Copyright © 1978 by Academic Press, Inc.
All rights of reproduction in any form reserved.

circulants is isomorphic to $R = F[x]/(\psi(x))$. We will identify this ring with the ring of circulants. Corresponding to the operation of matrix transpose there is a ring automorphism τ of R which has the properties (1) $\tau^2 =$ identity, (2) τ fixes the elements of F (i.e., the cosets of constant polynomials), and (3) τ inverts the coset $\bar{x}$ of x (i.e., T is orthogonal).

Thus in a general setting we suppose $R = F[x]/(\psi(x))$ is equipped with an automorphism τ with the three properties above and ask for the cardinality of the set $\text{Orth } \tau = \{a \in R \mid a\tau(a) = 1\}$.

R is an Artinian principal ideal ring and hence possesses a unique collection $\xi = \{e_i \mid 1 \leqslant i \leqslant r\}$ of idempotents with the properties (1) $e_i e_j = \delta_{ij} e_i$, (2) $\sum_{i=1}^{r} e_i = 1$, and (3) $e_i R$ is a local ring [1, p. 90]. Recall that a local ring is a ring with a unique maximal ideal. If $\psi(x)$ factors as $\psi(x) = f_1(x)^{n_1} \cdot f_2(x)^{n_2} \cdots f_r(x)^{n_r}$, where the $f_i(x)$ are distinct monic irreducibles of $F[x]$, then $e_i R$ is isomorphic to $F[x]/(f_i(x)^{n_i})$ if the indexing is suitable. We will identify $e_i R$ with the latter ring. Then the maximal ideal M_i of $e_i R$ is the ideal generated by the coset of $f_i(x)$ in $F[x]/(f_i^{n_i})$, the lattice of ideals of $e_i R$ is the sequence of powers $e_i R \supset M_i \supset M_i^2 \supset \cdots \supset M_i^{n_i} = 0$ of M_i and the multiplicity of f_i as a factor of $\psi(x)$ is the index of nilpotency of M_i.

Since an automorphism of R must simply permute the members of the set ξ we can decompose ξ into orbits of τ, $\{\xi_j \mid j \in J\}$. Then the ideal $S_j = \oplus_{e \in \xi_j} eR$ generated by a given orbit is a direct sum of local rings on each of which τ acts as an automorphism by restriction. In this way we study τ orbit by orbit. There is the corresponding Abelian group decomposition $\text{Orth } \tau \cong \prod_{j \in J} \text{Orth } \tau \mid_{S_j}$.

Since $\tau^2 = \text{id}$ then each orbit is either a 1-cycle $\{e_i\}$, where $\tau(e_i) = e_i$, or a 2-cycle $\{e_k, e_l\}$, where $\tau(e_k) = e_l$. Thus in the study of R and τ we may assume either (1) that R is local or (2) that $R = S \times T$, where S and T are isomorphic local rings and $\tau \mid_{S \times 0}$ and $\tau \mid_{0 \times T}$ are inverse isomorphisms.

The body of the paper is a study of the component direct summands of Orth τ which correspond to the 1-cycles and 2-cycles of τ. The analysis of these components is done in such a way as to provide a method for constructing all the orthogonal circulant matrices of order n over $GF(q)$. We give an explicit formula for the order $O(n, q)$ of the group of orthogonal circulant matrices of order n over $GF(q)$. (See Sect. 4.)

1. Reciprocal Polynomials

With the notation of the previous section we want to see how the notions of 1-cycle and 2-cycle of τ reveal themselves in the factorization of $\psi(x)$ over $F[x]$. First we define the basic terms of this section.

Definition. Let F be a field, $\psi(x)$ belong to $F[x]$, and let R be the ring

$F[x]/(\psi(x))$. If an automorphism τ of R has the three properties (1) $\tau^2 =$ identity, (2) τ fixes elements of F, and (3) τ inverts the coset of x, then we call τ the *transpose mapping of* R.

DEFINITION. A polynomial $\phi(x)$ of $F[x]$ is said to be reciprocal if $\phi(0) \neq 0$ and whenever α is a zero of $\phi(x)$ of multiplicity m, then also α^{-1} is a zero of $\phi(x)$ of multiplicity m.

Remark. The definition expresses the notion of reciprocal polynomial in terms appropriate to our point of view in this paper. However, a reciprocal polynomial is most easily recognized by the symmetry of its coefficients. That is, $\phi(x) = \sum_{i=0}^{k} a_i x^i$ is reciprocal if and only if $a_i = a_{k-i}$ for each i. (See [2], Vol. 1, p. 410.)

LEMMA 1. *If $R = F[x]/(\psi(x))$ has a transpose mapping, then $\psi(x)$ is reciprocal.*

Proof. R is a product of local rings associated one to one with the prime-power factors of $\psi(x)$. If we think of R in this way it is easy to see that the effect of τ is to produce an isomorphism from each factor onto another factor, because an automorphism will permute the set of local idempotents of R. Thus if f^l is one prime-power of $\psi(x)$, then τ produces an isomorphism from $F[x]/(f^l)$ onto $F[x]/(g^k)$, where g^k is another prime-power factor of $\psi(x)$. Since τ matches powers of the respective maximal ideals of these local rings one has $k = l$. Also, τ induces an isomorphism from $F[x]/(f)$ onto $F[x]/(g)$ and thus $\deg f = \deg g$. It is easy to prove from the properties of τ that this induced mapping takes $x + (f)$ to $(x + (g))^{-1}$ and fixes F. This says that if α is a root of f and β is a root of g there is an isomorphism from $F(\alpha)$ onto $F(\beta)$ which fixes F and maps α to β^{-1}. Then β^{-1} is a root of f. Thus the roots of f are the inverses of the roots of g. ∎

The following lemma is effectively the converse of Lemma 1.

LEMMA 2. *Let F be a field and f and g be irreducible polynomials of $F[x]$. Suppose that f and g have a common splitting field over F in which the roots of f and the roots of g are mutually reciprocal. Then for any fixed integer $l > 0$ there is a unique ring isomorphism τ from $F[x]/(f^l)$ onto $F[x]/(g^l)$ which fixes F and maps $x + (f^l)$ to $(x + (g^l))^{-1}$.*

Proof. Let π_f and π_g be the usual ring mappings from $F[x]$ onto $F[x]/(f^l)$ and $F[x]/(g^l)$, respectively. Since $(x, f) = 1$ and $(x, g) = 1$, then $\pi_f(x)$ and $\pi_g(x)$ are both invertible. Let ϕ denote the ring mapping from $F[x]$ into $F[x]/(g^l)$ induced by the usual embedding of F into $F[x]/(g^l)$ and the

assignment $x \to \pi_g(x)^{-1}$. Consider the commutative diagram of ring mappings

$$\begin{array}{ccc} F[x]/(g^l) & \xrightarrow{\pi} & F[x]/(g^l)/(\pi_g g) \\ {\scriptstyle\phi}\uparrow & & \| \\ F[x] & \xrightarrow{\delta} & F[x]/(g) \end{array}$$

where π is the usual epimorphism and the vertical isomorphism is the usual one. Here, δ must be the mapping which fixes F and maps x to $(x + (g))^{-1}$. Then $\delta(f(x)) = f(\delta(x)) = f((x + (g))^{-1}) = 0$ since $x + (g)$ is a root of g. It follows that $\pi\phi(f(x)) = 0$ so that $\phi(f(x)) \in (\pi_g(g))$. Then $\phi(f^l) = 0$. It follows that ϕ induces a ring mapping τ from $F[x]/(f^l)$ to $F[x]/(g^l)$ which fixes F and maps $x + (f^l)$ to $(x + (g^l))^{-1}$.

By a symmetric argument there is a ring mapping ρ from $F[x]/(g^l)$ to $F[x]/(f^l)$ which fixes F and maps $x + (g^l)$ to $(x + (f^l))^{-1}$. But then τ and ρ are clearly inverse mappings. The uniqueness of τ is clear. ∎

As an immediate consequence of the two above lemmas we have the following result.

THEOREM 1. *Let F be a field and $\psi(x) \in F[x]$. The ring $R = F[x]/(\psi(x))$ has a transpose mapping if and only if $\psi(x)$ is reciprocal.*

Proof. The "only if" is clear from Lemma 1 and the "if" is seen by decomposing R into local rings and using Lemma 2 to construct τ. ∎

In view of the above the following theorem is obvious.

THEOREM 2. *In the factorization of $\psi(x)$ a 1-cycle is associated with an irreducible reciprocal factor and a 2-cycle is associated with two nonreciprocal irreducible factors f and g of equal degree such that $f(x) \cdot g(x)$ is reciprocal.* ∎

In the study of 1-cycles of τ in the next section, a special case is made if the field automorphism τ_1 induced by τ is the identity mapping. In terms of the factors of $\psi(x)$ it is easy to determine if this happens.

LEMMA 3. *The induced automorphism $\tau_1 : F[x]/(f) \to F[x]/(f)$ at a 1-cycle is the identity if and only if $f(x)$ is either $x + 1$ or $x - 1$.*

Proof. Let $(^-)$ denote coset modulo f. Since $\bar{x}\tau_1(\bar{x}) = \bar{1}$ then if $\tau_1 = id$ one has $\bar{x}^2 = \bar{1}$ (i.e., $f \mid x^2 - 1$) so that either $f(x) = x + 1$ or $f(x) = x - 1$. The converse is obvious since τ fixes F and $\tau = \tau_1$ when $f(x)$ is either $x + 1$ or $x - 1$. ∎

Remark. If $f(x)$ is an irreducible reciprocal polynomial and $f(x)$ is not $x + 1$ or $x - 1$ then $f(x)$ has degree $2s$ for some positive integer s.

2. Orth τ at a 1-Cycle

Let R be $F[x]/(f(x)^m)$ where $f(x)$ is an irreducible reciprocal polynomial of $F[x]$ and let τ be the transpose mapping of R. Let M be the maximal ideal of R. On each homomorphic image R/M^i of R, τ induces an automorphism τ_i so that the following diagram commutes:

$$\begin{array}{lll}
R/M & \xrightarrow{\tau_1} & R/M \qquad \text{Level 1} \\
\uparrow & & \uparrow \\
R/M^2 & \xrightarrow{\tau_2} & R/M^2 \qquad \text{Level 2} \\
\uparrow & & \uparrow \\
\vdots & & \vdots \qquad \vdots \\
\uparrow & & \uparrow \\
R = R/M^m & \xrightarrow[\tau_m = \tau]{} & R/M^m = R \qquad \text{Level } m
\end{array}$$

τ_i is defined by $\tau_i(r + M^i) = \tau(r) + M^i$. The vertical maps are the usual epimorphisms. We will identify rings via the obvious isomorphisms $R/M^i \simeq F[x]/(f(x)^i)$. Of course τ_i is the transpose mapping of R/M^i and we will refer to Orth $\tau_i = \{a \in R/M^i \mid a\tau_i(a) = 1\}$, $i = 1, 2, \ldots, m$. We note that the vertical mappings induce group homomorphisms from Orth τ_{i+1} to Orth τ_i for $1 \leqslant i \leqslant m - 1$.

Orth τ_1 is relatively easy to determine since R/M is a field. If we knew that the mapping from Orth τ_m = Orth τ to Orth τ_1 was onto, then finding the order of Orth τ would be equivalent to finding the order of the kernel of this mapping. We will now investigate the level-by-level construction of an element of Orth τ which has the corollary that this mapping *is* onto, and provides an easy counting scheme.

We will think of R/M^i as the set of polynomials in $F[x]$ of degree less than the degree of $f^i(x)$ with their usual addition and with multiplication done modulo $f^i(x)$ as usual. In this way we have all the R/M^i as subsets of R. A polynomial $g(x)$ of R has a unique f-adic representation, i.e., $g(x) = \sum_{j=0}^{m-1} g_j(x) f^j(x)$, where the coefficients $g_j(x)$ belong to R/M. We shall always suppose that the elements of R/M^i are represented f-adically. Note that $g(x)$ is a unit of R/M^i if and only if $g_0(x) \neq 0$.

We want to know when $g(x) = \sum_{j=0}^{m-1} g_j f^j$ belongs to Orth τ = Orth τ_m. It is clear that if $g \in$ Orth τ, then for each $r < m$, $\sum_{j=0}^{r-1} g_j f^j \in$ Orth τ_r since the mapping from Orth τ to Orth τ_r amounts to a simple truncation of the f-adic representation. In particular $g_0 \in$ Orth τ_1, $g_0 + g_1 f \in$ Orth τ_2, and so on. To construct an element of Orth τ one selects first an element g_0 of Orth τ_1. Then one must find g_1 in R/M so that $g_0 + g_1 f$ is in Orth τ_2, etc.

The best that can happen is that having found $g_0, \ldots, g_{i-1}$ so that $\sum_{j=0}^{i-1} g_j f^j$ belongs to Orth τ_i one can always find g_i so that $\sum_{j=0}^{i} g_j f^j$ is in Orth τ_{i+1}. In fact, this is almost always possible, the only exception occurring when the characteristic of F is 2 and $f(x) = x + 1$.

DEFINITION. Let $g(x)$ belong to R. Suppose $g\tau(g) - 1$ has f-adic representation $g\tau(g) - 1 = \sum_{j=0}^{m-1} d_j f^j$. Then we call d_j *the jth deviation of* g.

Thus if $g \in R/M^i$ and $g \in$ Orth τ_i then we seek a $g_i \in R/M$ so that $g + g_i f^i$ has zero ith deviation, i.e., we want $g + g_i f^i$ to belong to Orth τ_{i+1}.

Since τ is an automorphism of R and f generates the maximal ideal of R, then also $\tau(f)$ generates the maximal ideal. Thus $\tau(f) = uf$ for some unit u of R. We let u_0 be the canonical image of u in R/M.

LEMMA 4. *If u_0 is the canonical image of u in R/M then u_0 belongs to Orth τ_1.*

Proof. Applying τ to $\tau f = uf$ one has $f = \tau(u)\, uf$ or $(u\tau(u) - 1)f = 0$. Since $f \neq 0$ then $u\tau(u) - 1$ is not a unit. Since R is local, $u\tau(u) - 1 \in M$ so that $u\tau(u) = 1 \bmod f$, which is the same as $u_0\tau_1(u_0) = 1$ in R/M. ∎

LEMMA 5. *Suppose that $g = \sum_{j=0}^{i-1} g_j f^j$ belongs to* Orth τ_i. *A necessary and sufficient condition for $g + g_i f^i$ to belong to* Orth τ_{i+1} *is that g_i satisfy*

$$\tau_1(g_i g_0^{-1})\, u_0^{\,i} + (g_i g_0^{-1}) = -d_i\,, \qquad (*)$$

where d_i is the ith deviation of g.

Proof. Calculating modulo f^{i+1}, the orthogonality condition

(a) $(g + g_i f^i)\, \tau(g + g_i f^i) = 1$

is easily reduced to

(b) $(d_i + g_i\tau(g) + g\tau(g_i)\, u^i) f^i = 0 \bmod f^{i+1}$.

This means

(c) $d_i + g_i\tau(g) + g\tau(g_i)\, u^i = 0 \bmod f$.

Since $\tau_1(g_0) = g_0^{-1} \bmod f$ the equivalence of (c) with (*) is obvious. ∎

We pause to examine $\tau_1 : R/M \to R/M$. Since $\tau_1^2 =$ identity then either τ_1 has order two or $\tau_1 =$ identity. Note that if F_1 denotes the fixed field of τ_1 in R/M then the mapping $\tau_1 +$ id is an F_1-linear endomorphism of R/M. The proofs of the various parts of the following lemma are elementary. Note that part (3) is a simple consequence of the Hilbert "Satz 90."

LEMMA 6. (1) *Except when* $\tau_1 = \mathrm{id}$ *and* Char $F = 2$ *we have* $\mathrm{Ker}(\tau_1 + \mathrm{id}) = \mathrm{Sk}\,\tau_1 = \{z \in R/M \mid \tau_1(z) = -z\}$ *and* $\mathrm{Im}(\tau_1 + \mathrm{id}) = F_1 =$ *fixed field of* τ_1. (2) $\mathrm{Sk}\,\tau_1 = zF_1$ *for some* z. (3) *The mapping* $z \to z^{-1}\tau_1(z)$ *from* $(R/M)^*$ *to* Orth τ_1 *is onto unless* $\tau_1 = \mathrm{id}$ *and* Char $F \neq 2$. ∎

By Lemma 4, $u_0 \in \mathrm{Orth}\,\tau_1$. Thus when $\tau_1 \neq \mathrm{id}$, part (3) of Lemma 6 furnishes us with an element β in R/M with the property that $\beta^{-1}\tau_1(\beta) = u_0^{-1}$. The β will have this fixed meaning when $\tau_1 \neq \mathrm{id}$. The following result is immediate.

THEOREM 3. *Assume* $\tau_1 \neq \mathrm{id}$. *Then with* β *as above, condition* (*) *is equivalent to*

$$(\tau_1 + \mathrm{id})(g_i/g_0\beta^i) = -d_i/\beta^i. \quad \blacksquare \qquad (**)$$

Apparently when $\tau_1 \neq \mathrm{id}$, a choice for g_i exists only if d_i/β^i belongs to $\mathrm{Im}\,(\tau_1 + \mathrm{id}) = F_1$, i.e., $\tau_1(d_i/\beta^i) = d_i/\beta^i$. We shall see that this is always so.

THEOREM 4. *Assume* $\tau_1 \neq \mathrm{id}$. *If* $g(x) \in \mathrm{Orth}\,\tau_i$, *then there is a* $g_i \in R/M$ *so that* $g + g_i f^i \in \mathrm{Orth}\,\tau_{i+1}$. *The number of choices of* g_i *is* $|F_1|$, *where* F_1 *is the fixed field of* τ_1 *in* R/M.

Proof. We must show that $\tau_1(d_i/\beta^i) = d_i/\beta^i$. Since $g\tau(g) = 1 + d_i f^i \bmod f^{i+1}$, then applying τ we have $g\tau(g) = 1 + u^i\tau(d_i) f^i$. Thus $u^i\tau(d_i) = d_i \bmod f$, i.e., $u_0{}^i\tau_1(d_i) = d_i$. Then since $\tau_1(\beta) = \beta/u_0$ one has $\tau_1(d_i/\beta^i) = \tau_1(d_i)\,\tau_1(\beta)^{-i} = \tau_1(d_i)\,u_0{}^i\beta^{-i} = d_i/\beta^i$.

The number of choices of g_i can be seen from (**) to be equal to the cardinality of $\mathrm{Ker}(\tau_1 + \mathrm{id}) = \mathrm{Sk}\,\tau_1$ and since $\mathrm{Sk}\,\tau_1 = zF_1$ for some z then this number is $|\mathrm{Sk}\,\tau_1| = |F_1|$. ∎

In case $F = GF(q)$ we have the following counting theorem.

COUNT 1. *Let* $F = GF(q)$. *If* $f(x)$ *is an irreducible reciprocal* (1*-cycle*) *factor of* $\psi(x)$ *of multiplicity* m *and degree* $2s$ *then the corresponding orthogonal group component has order*

$$(q^s + 1)\, q^{s(m-1)}.$$

Proof. τ_1 is an automorphism of $GF(q^{2s}) = F[x]/(f)$ over F of order 2. Thus $\tau_1(z) = z^q$ for each z in $GF(q^{2s})$. Then Orth $\tau_1 = \{z \in GF(q^{2s}) \mid z \cdot z^{q^s} = 1\} = \{z \mid z^{q^s+1} = 1\}$. Thus Orth τ_1 is the unique subgroup of $GF(q^{2s})^*$ of order $q^s + 1$. The fixed field F_1 of τ_1 is $GF(q^s)$. The count is now an easy consequence of Theorem 4. ∎

EXAMPLE. For 12×12 circulants over $GF(2)$ one has the factorization $x^{12} - 1 = (x^3 - 1)^4 = (x + 1)^4(x^2 + x + 1)^4$, where both irreducible factors

are reciprocal. Orth τ is the direct product of two component groups. The component corresponding to $f(x) = x^2 + x + 1$ has order $3 \cdot 2^3 = 24$.

It remains to see what occurs when $\tau_1 = \mathrm{id}$. That is, what is the nature of the construction of orthogonal elements at a 1-cycle where $f(x) = x + 1$ or $f(x) = x - 1$? Since we have specific $f(x)$ we can be more explicit about the quantity u_0 appearing in Eq. (*). We have

$$\begin{aligned}\tau(f) &= \tau(x \pm 1) = x^{-1} \pm 1 = (\mp 1 + f)^{-1} \pm 1 \\ &= (\mp 1 - f \mp f^2 - f^3 \mp \cdots) \pm 1 \\ &= -f \mp f^2 - f^3 \mp \cdots \\ &= (-1 \mp f - f^2 \mp \cdots) f.\end{aligned}$$

Hence $u = -1 \mp f - f^2 \mp \cdots$ and $u_0 = -1$. Then (*) becomes

$$(g_i g_0^{-1})(1 + (-1)^i) = d_i \,. \tag{***}$$

If $g = g_0 + g_1 f + \cdots + g_{i-1} f^{i-i}$ is in Orth τ_i for some *odd* i, it is possible to find g_i so that $g + g_i f^i$ is in Orth τ_{i+1} *only if* $d_i = 0$, i.e., only if already $g \in$ Orth τ_{i+1}, in which case the choice of g_i is a free one in F. The next theorem shows that for odd i, d_i is in fact zero.

THEOREM 5. *Let $f(x)$ be $x + 1$ or $x - 1$. If $j \geqslant 0$ is even and $g(x)$ belongs to* Orth τ_{j+1}, *then also $g(x)$ belongs to* Orth τ_{j+2}.

Proof. Suppose $g \in$ Orth τ_{j+1} for some even $j \geqslant 0$. We wish to show that g has zero $(j+1)$st deviation so that $g \in$ Orth τ_{j+2}.

One has from $g \in$ Orth τ_{j+1} that

$$g\tau(g) = 1 + bf^{j+1} + cf^{j+2} + \cdots. \tag{1}$$

Apply τ to get

$$g\tau(g) = 1 + b(\tau f)^{j+1} + c(\tau f)^{j+2} + \cdots.$$

Since $\tau f = -f \mp f^2 - f^3 \mp \cdots$, then (2) yields

$$g\tau(g) = 1 + b(-f^{j+1} \mp (j+1) f^{j+2}) + cf^{j+2} + \cdots, \tag{3}$$

or equivalently

$$g\tau(g) = 1 - bf^{j+1} + (c \mp (j+1)\, b) f^{j+2} + \cdots. \tag{4}$$

Comparing (1) and (4) we have

$$\begin{aligned} b &= -b, \\ (j+1)\, b &= 0. \end{aligned} \tag{5}$$

If Char $F = 2$, then $b = 0$ from the second equation of (5) and if Char $F \neq 2$, then $b = 0$ from the first equation. In any case $b = 0$ and so $g \in \text{Orth } \tau_{j+2}$. ∎

It follows from (***) and this theorem that there is no difficulty in constructing an element of Orth τ at odd levels. In fact the choice of g_i for odd i is unrestricted and may be any member of $R/M = F$. When i is even and Char $F \neq 2$ then (***) has a unique solution $g_i = -d_i g_0/2$. Thus the following counting theorem is immediate.

COUNT 2. *Assume that $F = GF(q)$, $q = p^l$, $p \neq 2$. At a 1-cycle corresponding to a factor $f(x) = x + 1$ or $f(x) = x - 1$ of multiplicity m of $\psi(x)$ the orthogonal group component has order $2q^{[m/2]}$.* ∎

There remains the case $f(x) = x + 1$ when Char $F = 2$. Since in this case Orth $\tau_1 = \{1\}$ then $g_0 = 1$ and by Theorem 5, g_1 is an arbitrary choice in F. Having chosen g_1 it is *not* always possible to find a g_2 in F so that $g_0 + g_1 f + g_2 f^2 \in \text{Orth } \tau_3$. In fact only if g_1 is either 0 or 1 does an appropriate g_2 exist. The situation is described in the following theorem.

THEOREM 6. *Suppose that $f(x) = x + 1$ and* Char $F = 2$. *Of the $|F|$ choices for g_1 only the choices $g_1 = 0$ and $g_1 = 1$ permit a choice of g_2. Beyond this if $g \in \text{Orth } \tau_i$ for some odd i, $i > 1$, then $g \in \text{Orth } \tau_{i+1}$ and of the $|F|$ choices of g_i only the choice where g_i is the ith deviation of g will allow a choice of g_{i+1}. The choice of g_{i+1} is then a free one in F.*

Proof. Suppose beginning with 1 in Orth τ_1 we ask for a_1 and a_2 in F so that $g = 1 + a_1 f + a_2 f^2$ belongs to Orth τ_3.

Using

$$\tau f = f + f^2 + f^3 + \cdots \tag{6}$$

one has

$$\tau g = 1 + a_1 f + (a_1 + a_2) f^2 + \cdots. \tag{7}$$

From (7) one finds that

$$g\tau(g) = 1 + (a_1 + a_1^2) f^2 + \cdots. \tag{8}$$

Thus $g \in \text{Orth } \tau_3$ if and only if $a_1 + a_1^2 = 0$ in F, i.e., $a_1 = 0$ or $a_1 = 1$. This proves the first statement.

Now suppose that $g = 1 + a_1 f + \cdots + a_{i-1} f^{i-1}$ belongs to Orth τ_i for some odd i, $i > 1$. We seek a_i and a_{i+1} in F so that $h = g + a_i f^i + a_{i+1} f^{i+1}$ belongs to Orth τ_{i+2}. We will work in R/M^{i+2}, i.e., modulo f^{i+2}.

From Theorem 5 we know that automatically $g \in \text{Orth } \tau_{i+1}$ so there is a $c \in R/M$, the $(i+1)$st deviation of g, so that

$$g\tau(g) = 1 + cf^{i+1}. \tag{9}$$

One has

$$\tau(h) = \tau(g) + a_i(\tau f)^i + a_{i+1}(\tau f)^{i+1} \tag{10}$$

and from (6) one finds

$$\tau(h) = \tau(g) + a_i f^i + (a_{i+1} + ia_i) f^{i+1}. \tag{11}$$

Since Char $F = 2$ one has

$$\tau(h) = \tau(g) + a_i f^i + (a_i + a_{i+1}) f^{i+1}. \tag{12}$$

From (12) one has

$$g\tau(h) = g\tau(g) + a_i f^i + [c + a_i(a_1 + 1) + a_{i+1}] f^{i+1}. \tag{13}$$

From (10) and the fact that $i \geqslant 3$ one has

$$h\tau(h) = g\tau(h) + a_i\tau(g) f^i + a_{i+1}\tau(g) f^{i+1} \tag{14}$$

and from (14) and (7) one has

$$h\tau(h) = g\tau(h) + a_i(1 + a_1 f) f^i + a_{i+1} f^{i+1}. \tag{15}$$

Combining (15) and (13) one has

$$h\tau(h) = 1 + (c + a_i) f^{i+1}. \tag{16}$$

Thus we see, having $g \in \text{Orth } \tau_i$, that even though $g + a_i f^i$ belongs to Orth τ_{i+1} for any $a_i \in F$ only for the choice $a_i = c$, the $(i + 1)$st deviation of g, can the construction proceed further. ∎

We can now complete our collection of counting theorems for 1-cycles.

COUNT 3. *Assume $F = GF(q)$, $q = p^l$, $p = 2$. If $f(x) = x + 1$ and has multiplicity m as a factor of $\psi(x)$ then the corresponding orthogonal group component has order*

$$\begin{array}{ll} 1 & \text{if } m = 1, \\ q & \text{if } m = 2, \\ 2q^{[m/2]} & \text{if } m > 2. \end{array}$$ ∎

3. ORTH τ AT A 2-CYCLE

Corresponding to a 2-cycle of τ one has a pair $f(x)$ and $g(x)$ of non-reciprocal irreducible factors of $\psi(x)$ of equal degree and multiplicity m so that $f(x) \cdot g(x)$ is reciprocal. This produces a factor $S \times T$ of the algebra

of circulants where $S \simeq F[x]/(f(x)^m)$ and $T = F[x]/(g(x)^m)$ on which τ acts so that $\tau|_{S\times 0}$ is inverse to $\tau|_{0\times T}$. We shall identify $S \times 0$ with S and $0 \times T$ with T so that if $s \in S$, then $\tau(s)$ has the obvious meaning. Since $\tau(s, t) = (\tau(t), \tau(s))$ then it is clear that an element (s, t) of $S \times T$ belongs to Orth τ if and only if s is invertible and $t = \tau(s)^{-1}$. The following theorem is clear.

THEOREM 7. *The mapping $s \mapsto (s, \tau(s)^{-1})$ is an isomorphism of the group of units S^* of S onto the orthogonal group component at the 2-cycle $S \times T$.* ∎

We can now complete our counting theorems on the various components of the orthogonal group.

COUNT 4. *Let $F = GF(q)$, $q = p^l$. For the 2-cycle pair $f(x)$ and $g(x)$ of factors of $\psi(x)$ of degree t and multiplicity m the corresponding orthogonal group component has the cardinality of the group of units of $F[x]/(f(x)^m)$, namely, $(q^t - 1)\, q^{t(m-1)}$.* ∎

4. THE NUMBER OF $n \times n$ ORTHOGONAL CIRCULANTS OVER $GF(q)$

In this section we exploit the properties of the particular reciprocal polynomial $\psi(x) = x^n - 1$. The previous results yield a count of the number of orthogonal circulants given the number of 1-cycles and 2-cycles occurring in the factorization of $\psi(x)$, together with their degrees and multiplicity. We indicate how this is found for a given n and q.

Factor $n = n_1 p^k$ so that $(n_1, p) = 1$. Then $x^n - 1 = (x^{n_1} - 1)^{p^k}$ and $x^{n_1} - 1$ has only simple zeros. Thus all 1-cycles and 2-cycles have the same multiplicity, p^k.

Next factor $x^{n_1} - 1 = \prod_{j|n_1} \Phi_j(x)$ into its cyclotomic factors. We claim that either Φ_j factors into irreducible reciprocal factors (1-cycles), or that Φ_j has no irreducible reciprocal factor, in which case it is clear that the irreducible factors of Φ_j may be paired so as to produce 2-cycles.

Recalling that the zeros of $\Phi_j(x)$ are the primitive jth roots of 1 it is easy to see that all the irreducible factors of Φ_j have the same degree. Say $\Phi_j = f_1 f_2 \cdots f_r$. If f_i is reciprocal of degree $2s$, then the automorphism τ_1 of the splitting field $GF(q^{2s}) = F[x]/(f_i)$ of f_i over F is the mapping $z \to z^{q^s}$ and τ_1 inverts each zero of f_i. A zero α of f_i is a primitive jth root of 1 so $\alpha^{-1} = \alpha^{q^s}$ is equivalent to $j \mid q^s + 1$. Conversely if $j \mid q^s + 1$ for some s and s is the least such positive integer, then $z \to z^{q^s}$ inverts each primitive jth root of 1. Then α has degree $2s$ and so f_i has degree $2s$ and is reciprocal. Since the condition $j \mid q^s + 1$ is independent of the choice of f_i we see that either all the factors of Φ_j are reciprocal or none is.

Since Φ_j has degree $\phi(j)$, where ϕ is the Euler ϕ-function, then we see that Φ_j factors into $\phi(j)/2s$ irreducible reciprocal polynomials of $F[x]$ of degree $2s$ if and only if $j \mid q^s + 1$ and s is the least such positive integer. We may express this last condition in the following equivalent way. Let $Z_j{}^*$ be the multiplicative group of units of the ring of integers modulo j. Then since q is prime to j, the residue class q_j of q modulo j belongs to $Z_j{}^*$. We denote by $[q_j]$ the cyclic subgroup of $Z_j{}^*$ generated by q_j. Then Φ_j factors into irreducible reciprocal polynomials of $F[x]$ if and only if $-1 \in [q_j]$, in which case the degree of each irreducible factor is the same as the order of the group $[q_j]$.

Of course Φ_j factors into nonreciprocal irreducible factors in $F[x]$ if and only if $-1 \notin [q_j]$. Then the factors of Φ_j all have degree t equal to the degree of any primitive jth root of 1 over F. Clearly t is the least positive integer so that $j \mid q^t - 1$, i.e., t is the order of the group $[q_j]$.

Our main counting theorem follows immediately from the theorems Count 1–4.

COUNTING THEOREM FOR ORTHOGONAL CIRCULANTS. *Denote by* $O(n, q)$ *the order of the group of orthogonal* $n \times n$ *circulants over* $GF(q)$, $q = p^l$. *Factor* $n = n_1 p^k$ *where* $(n_1, p) = 1$. *For* j *an integer prime to* p *let* $a = a(j, q)$ *denote the order of the subgroup* $[q_j]$ *in* $Z_j{}^*$ *and define* $O_j(n, q)$ *as follows*:

$$(j > 2)\colon O_j(n, q) = \begin{cases} [(q^{\frac{1}{2}a} + 1)\, q^{\frac{1}{2}a(p^k-1)}]^{\phi(j)/a} & \text{if } -1 \in [q_j], \\ [(q^a - 1)\, q^{a(p^k-1)}]^{\phi(j)/2a} & \text{if } -1 \notin [q_j], \end{cases}$$

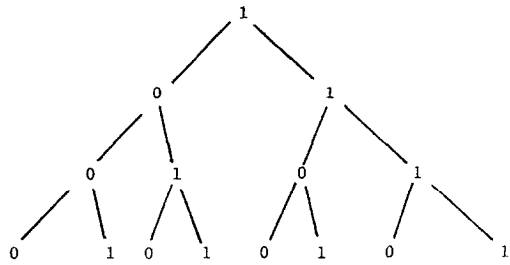
$$(j = 1, 2)\colon O_j(n, q) = \begin{cases} 2q^{\frac{1}{2}(p^k-1)} & \text{if } p \neq 2, \\ 1, \ k = 0 \\ q, \ k = 1 & \text{if } p = 2. \\ 2q^{2^{k-1}}, \ k > 1, \end{cases}$$

$$\text{Then } O(n, q) = \prod_{j \mid n_1} O_j(n, q).$$

5. CONSTRUCTION OF THE 12×12 ORTHOGONAL CIRCULANTS OVER $GF(2)$

In contrast to the counting, the construction requires the prime factorization of the polynomial $\psi(x) = x^n - 1$ over $F = GF(2)$. Here one has $x^{12} - 1 = (x^3 + 1)^4 = (x + 1)^4(x^2 + x + 1)^4$. So Orth $\tau \cong$ Orth $\tau' \times$ Orth τ'', where τ' and τ'' are the transpose mappings on $F[x]/(x + 1)^4$ and $F[x]/(x^2 + x + 1)^4$, respectively.

A. *Orth* τ'. Let $f(x) = x + 1$. The set Orth τ' can be displayed as a tree



where to every path in the tree from its top level to its bottom level there corresponds a unique element of Orth τ'. For instance to the path $\{1, 0, 1, 0\}$ corresponds the element of Orth τ' with those f-adic coefficients, namely $1 + 1(x + 1)^2 = x^2$. This tree is an immediate consequence of Theorem 6. Note that only one tree is needed here because Orth $\tau'_1 = \{1\}$. Usually we need a tree for each member of Orth τ_1.

B. *Orth* τ''. To construct members of Orth τ'' will require some knowledge of the quantity β appearing in Theorem 3 which governs this situation. The following lemma is then useful.

LEMMA 7. *If* $R = F[x]/f(x)^k)$, *where* $f(x)$ *is an irreducible reciprocal polynomial of* $F[x]$ *of degree* $2s$, *then one may take* $\beta = x^{-s} \bmod f$.

Proof. If $\bar{F}$ is a splitting field of $f(x)$ over F then the ring $\bar{R} = \bar{F}[x]/(f(x)^k)$ contains R and the transpose $\bar{\tau}$ of $\bar{R}$ extends the transpose τ of R. In $\bar{F}[x]$ one has $f(x) = \prod_{\alpha\in\Lambda}(x - \alpha)(x - \alpha^{-1})$ where Λ is a set of s roots of $f(x)$ no two of which are reciprocal. Then

$$\tau(f) = \bar{\tau}(f) = \prod_{\alpha\in\Lambda}(x^{-1} - \alpha)(x^{-1} - \alpha^{-1})$$

so that

$$x^{2s}\tau(f) = \prod_{\alpha\in\Lambda}(1 - \alpha x)(1 - \alpha^{-1}x) = \prod_{\alpha\in\Lambda}(x - \alpha)(x - \alpha^{-1}) = f.$$

It follows that since $\tau f = uf$ then $u = x^{-2s} \bmod f$.
Then taking $\beta = x^{-s} \bmod f$ one has

$$\beta^{-1}\tau_1(\beta) = x^s\tau_1(x^{-s}) = x^s \cdot x^s = x^{2s} = u^{-1} \bmod f. \quad \blacksquare$$

Clearly Orth τ''_1 is the group $GF(4)^* = F[x]/(x^2 + x + 1)^* = \{1, x, x + 1\}$. From the above $\beta = x^{-1} = x + 1$.

Let $f(x) = x^2 + x + 1$. By reference to (**) and Theorems 3 and 4

we find that for an element g in Orth τ_i with ith deviation d_i the choices of g_i are to be made from the set $g_0(d_i x + \beta^i F)$ modulo f. Note that here $\mathrm{Ker}(\tau_1'' + \mathrm{id}) = \mathrm{Sk}\,\tau_1'' = F_1$, the fixed field of τ_1'' in $GF(4)$ so $F_1 = F = GF(2)$.

For instance, with $g_0 = 1$ the first deviation is clearly 0 so that the desired tree has as its second level vertices the members of the set $\beta F = \{x + 1, 0\}$.

In order to find deviations we find via the division algorithm that

$$\tau''(x) = x^{-1} = x^7 + x^3 = (x + 1) + (x + 1)f + (x + 1)f^2 + (x + 1)f^3$$

and hence

$$\tau''(x^2) = \tau''(x)^2 = x + f + xf^2 + f^3$$

and

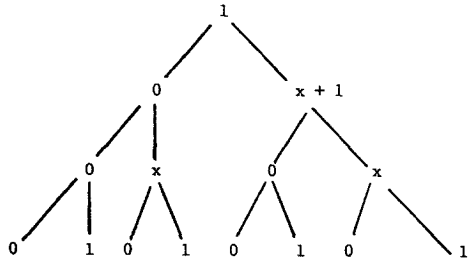
$$\tau''(f) = xf + f^2 + xf^3.$$

To extend the path $\{1, x + 1\}$ to the next level we need the second deviation of $g = 1 + (x + 1)f$. We calculate

$$\tau''(g) = 1 + \tau''(x + 1)\,\tau''(f) = 1 + (x + 1)f + xf^2$$

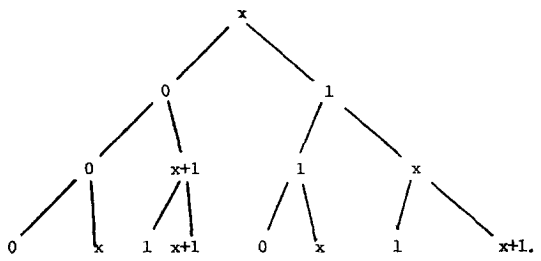
and then $g\tau''(g) = 1$ so that g has zero second deviation. Thus the path $\{1, x + 1\}$ extends by choosing the vertices in $\beta^2 F = \{0, x\}$ at the third level.

The tree

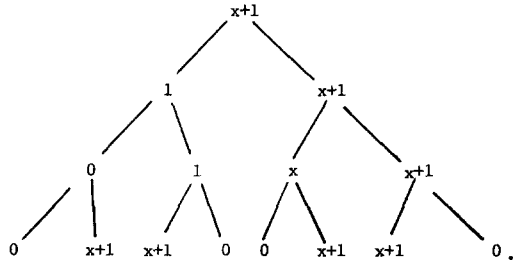


displays the completed tree for the choice $g_0 = 1$ in Orth τ_1''. This is the kernel of the canonical mapping from Orth τ'' onto Orth τ_1''.

It follows that the corresponding tree for the choice $g_0 = x$ can be found by multiplying the tree for $g_0 = 1$ by any one completed path from x. The easy choice is $\{x, 0, 0, 0\}$. This yields



Similarly for $x + 1$ one has



These three trees describe the elements of Orth τ''.

Then to construct a particular 12×12 orthogonal circulant one finds the local idempotents. Since $1 = x(x + 1) + (x^2 + x + 1)$ then the local idempotents of $F[x]/(x^{12} - 1)$ are $e' = (x^2 + x + 1)^4$ and $e'' = (x^2 + x)^4$. Then selecting the path $(1, 0, 1, 1)$ of Orth τ' and the path $(x, 1, 1, x)$ of Orth τ'' we compute $e'(1, 0, 1, 1) + e''(x, 1, 1, x)$. That is, $(x^2 + x + 1)^4[1 + (x + 1)^2 + (x + 1)^3] + (x^2 + x)^4[x + (x^2 + x + 1) + (x^2 + x + 1)^2 + x(x^2 + x + 1)^3]$ or $1 + x + x^2 + x^4 + x^6 + x^7 + x^8$ which yields the circulant whose first row is $(1, 1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0)$.

6. Concluding Remarks

(1) Sections 1–3 are applicable to any algebra of the kind $F[x]/(\psi(x))$, where $\psi(x)$ is a reciprocal polynomial. For instance, once could apply them to count and construct orthogonal matrices within the algebra $F[A]$ generated by any given orthogonal matrix A.

(2) There is another construction procedure which uses the splitting field of $\psi(x)$, and some elementary Galois theory. In this procedure one need not find the local idempotents and the calculation of deviations is replaced by the task of solving certain equations in the splitting field.

(3) The sets of symmetric circulants or skew ones can be constructed by making a few changes in the above. For instance if the a, n_1, k have the same meaning as before then one can prove the following.

Count of Invertible Symmetric Circulants. *Let $S(n, q)$ be the number of $n \times n$ symmetric invertible circulatns over $GF(q)$. For j prime to q define $S_j(n, q)$ as follows*:

$$j > 2\colon S_j(n, q) = \begin{cases} [(q^{\frac{1}{2}a} - 1)\, q^{\frac{1}{2}a(p^k-1)}]^{\phi(j)/a} & \text{if } -1 \in [q_j], \\ [(q^a - 1)\, q^{a(p^k-1)}]^{\phi(j)/2a} & \text{if } -1 \notin [q_j], \end{cases}$$

$$j = 1, 2\colon S_j(n, q) = \begin{cases} (q-1)q^{\frac{1}{2}(p^k-1)} & \text{if } p \neq 2, \\ \begin{cases} q - 1 & \text{if } k = 0, \\ q(q-1) & \text{if } k = 1, \\ (q-1)\, q^{2^{k-1}} & \text{if } k > 1, \end{cases} & \text{if } p = 2. \end{cases}$$

$$\textit{Then } S(n, q) = \prod_{j \mid n_1} S_j(n, q).$$

References

1. M. F. Atiyah and I. G. McDonald, "Introduction to Commutative Algebra," Addison–Wesley, Reading, Mass., 1969.
2. G. Chrystal, "Textbook of Algebra," 7th ed., Chelsea, New York, 1964.
3. F. J. MacWilliams, Orthogonal circulant matrices over finite fields and how to find them, *J. Combinatorial Theory* **10** (1971), 1–17.